Scientific Research Publishing

Journal of Information Security, 2018, 9, 85-94
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Security Analysis of Subspace Network Coding

Yantao Liu[1], Yasser Morgan[2]

[1]College of Engineering, Bohai University, Jinzhou, China
[2]Faculty of Engineering and Applied Science, University of Regina, Regina, Canada
Email: liuyantaocn@163.com

How to cite this paper: Liu, Y.T. and Morgan, Y. (2018) Security Analysis of Subspace Network Coding. *Journal of Information Security*, **9**, 85-94.
https://doi.org/10.4236/jis.2018.91007

Received: December 25, 2017
Accepted: January 20, 2018
Published: January 23, 2018

Abstract

This paper analyzed the security of constant dimensional subspace code against wiretap attacks. The security was measured in the probability with which an eavesdropper guessed the source message successfully. With the methods of linear algebra and combinatorics, an analytic solution of the probability was obtained. Performance of subspace code was compared to several secure network coding schemes from the perspective of security, flexibility, complexity, and independence, etc. The comparison showed subspace code did not have perfect security, but it achieved probabilistic security with low complexity. As a result, subspace code was suitable to the applications with limited computation and moderate security requirement.

Keywords

Network Security, Wiretap Attacks, Subspace Code, Network Coding

1. Introduction

Wiretap attacks on networks denote an eavesdropper, named by *Eve*, intends to resolve the source message by wiretapping network transmissions. A wiretap attack is imperceptible since it does not disturb normal communications. For a communication network, the security performance against wiretap attacks is tightly related to the underlying transmission mechanisms. There are two types of transmission mechanisms of communication networks: routing and network coding. Traditional routing networks operate in the way of store and forward. A relay node is only allowed to faithfully forward the received packets. Accordingly, if *Eve* intercepts a routing packet, he will obtain the containing message. On the contrary, a linear network coding (LNC) system operates in the way of store, encode, and forward. In the LNC realm, an intermediate node is allowed to combine received packets to generate and pass on novel output packets. As a result, if *Eve* intercepts a LNC packet, he cannot resolve the source message except

he can successfully decode. Two necessities are required for successful LNC decoding by a legal subscriber or *Eve* [1]:

- Enough received packets.
- Full knowledge of coding rules, such as local coding vectors (LCV) or global coding vectors (GCV).

Both necessities demand stronger capabilities with *Eve* in LNC networks than in routing networks. Thus, LNC is inherently more secure than routing. In this paper, we name the intrinsic secure nature of LNC by *basic security*. An example of routing and LNC is shown in **Figure 1**.

Definition 1. (Wiretap Network Model) [2]: The wiretap network model (WNM) is a quadruple (G, S, R, A).

- A directed acyclic graph $G = (V, E)$, with V and E representing the sets of nodes and edges, respectively.
- A source node $S \in V$.
- A set of receiver nodes $R = \{r_i : r_i \in V\}$.
- A collection of wiretap channel sets $A = \{A : A \subset E\}$. An enemy can wiretap only one instance of A.

If the number of wiretapped edges is limited, say $|A| \leq r$, *i.e.*, there are r wiretapped edges at most, but the wiretap pattern A is not fixed, it is called r-WNM [3].

Based on WNM or r-WNM, a variety of secure LNC schemes were proposed. According to the protection strength, we classify these schemes into three security grades: *weak security*, *perfect security* and *strong security*. Let $\mathbf{m} = (m_1, \cdots, m_n)$ and $\mathbf{y}_A$ denote the source message and the set of symbols intercepted from the wiretap pattern A, respectively. Then, weak security [4] aims to protect a source symbol m_i from being solved. There are two classes of weakly secure LNC schemes. The first depends on an elaborately designed LNC algorithm [4] [5]. Its basic idea is to force the symbol on network links to be a mixture of $(m_1, \cdots, m_n)$ so that the knowledge of $\mathbf{y}_A$ with $|A| < n$ is not enough to solve m_i. The second leverages classical cryptography to protect message by encryption [6] [7] [8] [9]. Moreover, [10] developed a weakly secure random linear network coding scheme based on the approach of one-time pad. To reduce the security which is then generalized seamlessly to inter-generation coding. Perfect security [12] aims overhead, Liu *et al.* [11] proposed

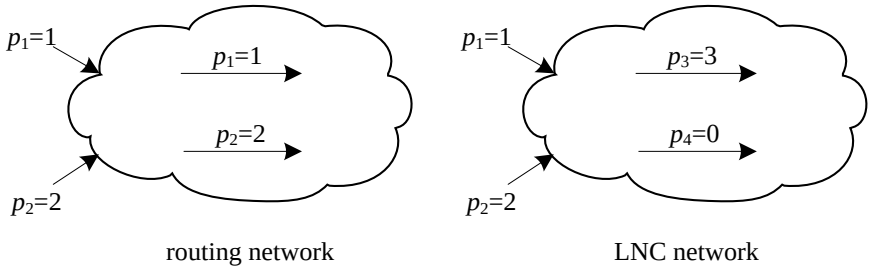

Figure 1. A comparison between routing network and LNC network. The LNC is defined over F_5 and the coding rule is $p_3 = l_{11}p_1 + l_{12}p_2 = 1 \times 1 + 1 \times 2 = 3$, $p_4 = l_{21}p_1 + l_{22}p_2 = 1 \times 1 + 2 \times 2 = 0$.

an intra-generation coding encryption models to protect the information of $\mathbf{m}$ from leakage, *i.e.*, $H(\mathbf{m}|\mathbf{y}_A) = H(\mathbf{m})$. A perfectly secure LNC scheme can be built based on precoding [3] [12], coset code [13], or rank metric code [14]. Strong security [15] improves perfect security by reducing information leakage in case that perfect security is broken.

A comparison between perfect security and weak security is shown in **Figure 2**. **Figure 2(a)** shows a case of $r = 1$ perfect security. The message $\mathbf{m}$ consists of a symbol x over the finite field of F_3. It is concealed by a random symbol k. No matter which edge (upper or lower, but not both) is wiretapped, *Eve* gets no information about x. **Figure 2(b)** is an example of $r = 1$ weak security. The source message $\mathbf{m}$ is composed of two symbols x_1 and x_2 over F_3. It is easy to check that with only one symbol overheard from any edge, *Eve* can get an amount of information about $\mathbf{m} = (x_1, x_2)$, but he cannot guess the value of x_1 or x_2 precisely.

In this paper, we aim to analyze the security performance of subspace code against wiretap attacks. Subspace code is a kind of source coding strategy combined with random LNC. It was utilized and analyzed by Kötter and Kschischang [16] for error correction. But the security performance of subspace code against wiretap attacks, to the best of our knowledge, is still missing. This paper addresses the basic security of subspace code. That is to say only a raw LNC system using subspace code is considered and no extra mechanisms, such as encryption or source coding, are included. With the method of combinatorics, we calculate the probability with *Eve* to precisely guess the sending message by wiretapping packets from network links. To the best of our knowledge, this is the first quantitative analysis being done on the security performance of subspace network coding against wiretap attacks so far.

The remainder of the paper is organized as the following: Section II introduces the concept of subspace code and its application on error correction; Section III presents detailed analysis to the security of subspace code against wiretap attacks. Some quantitative results are obtained; In Section IV, we compared subspace code with several LNC schemes; Finally, we summarize the conclusion in Section V.

2. Subspace Code

Subspace code belongs to the family of array code [17], which represents messages by matrices. Instead of mapping a message into a scalar or a vector, subspace De-note the overall space over the finite field F_q by F_q^n. See **Figure 3** as an example. code represents a source message by a subspace of a given n-dimensional space.

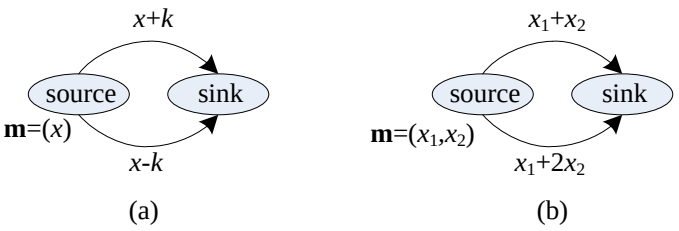

Figure 2. Perfect security and weak security. (a) perfect security; (b) weak security.

The overall space is F_5^4. Figure 3 shows the transmission of the message 'A' as an example. When the source node S sends 'A', it maps 'A' into the 3-dimensional subspace spanned by {(1000), (0100), (0010)} and injects the three basis vectors into the network. After the transportation with random LNC, a sink node R receives three independent vectors, say {(1000), (0020), (0300)}. It decodes 'A' by identifying the corresponding subspace.

Subspace code is based on the vector space preserving property of LNC [16]. If the dimension of subspaces is constant for all code words in a codebook, it is called constant dimensional subspace code. This type of code plays an important role in subspace code due to low complexity of encoding and decoding. Subspace code fulfills noncoherent communications, *i.e.*, the source and sink nodes do not need to care about the network topology, so it is very suitable for a topology variable network.

Kötter and Kschischang [16] utilized subspace code to make error and erasure control for random LNC. They modeled a random LNC system as a subspace operator channel, whose input and output are two subspaces U and V, respectively. In the context of constant dimension code, U and V are both k dimensional subspaces of F_q^n. Due to errors and/or erasures, U and V may be different. To make error correction, Kötter and Kschischang defined a subspace distance metric $d_S(U,V)$ as

$$d_S(U,V) = \dim(U+V) - \dim(U \cap V) \tag{1}$$

where the sum space $U+V = \{u+v : u \in U, v \in V\}$ is the smallest subspace containing both U and V, and the intersection space $U \cap V$ is the biggest subspace contained in both U and V. A minimum distance decoding rule is defined in terms of $d_S(U,V)$.

$$\hat{V} = \underset{V \in \text{ code book}}{\arg\min}\ d_S(U,V) \tag{2}$$

If subspace code is implemented in a hostile environ, the designer and users may care about its security performance against various attacks. In this paper, we address the security of subspace code against wiretap attacks.

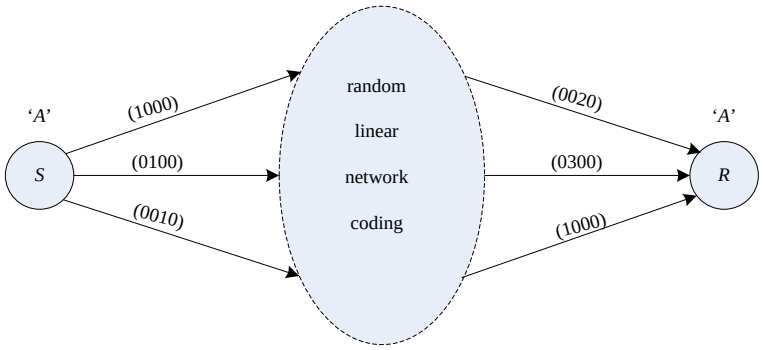

Figure 3. An example of subspace coding. The message 'A' is encoded into a subspace spanned by {(1000), (0100), (0010)}. After transmission with the random LNC network, the sink R received three vectors {(1000), (0300), (0020)}, which spans the same subspace to the one spanned by {(1000), (0100), (0010)}, so R decodes the message 'A' by identifying the subspace.

3. Security Analysis of Subspace Code

In a random LNC network [18], LCVs are generated locally and randomly at intermediate nodes during transmission, and GCVs are attached with code words in the packets. If a packet is intercepted, the code words and corresponding GCV will be exposed simultaneously, so random LNC is potentially weak. Subspace code takes a random LNC network as the underlying transportation. But in a subspace code network, receivers do not depend on GCVs to decode, so that only code words are contained in packets. From this point, subspace code is superior to random LNC against wiretap attacks. Next, we make detailed analyses to the security of subspace code against wiretap attacks.

3.1. System Model

Consider an error free random LNC network using k dimensional subspace code over F_q^n. The eavesdropper *Eve* wiretaps l network links and tries to restore the source message. Assume *Eve* masters the full knowledge of the subspace code, *i.e.*, he knows the finite field F_q, the dimension parameters n and k, and the code book, etc. Thus, *Eve* behaves just like a valid subscriber except that he can only collect l vectors from the network. Obviously, l measures his wiretap capability. Specifically, if $l = k$, he can decode the source message just like a legal subscriber; If $l < k$, the number of intercepted packets is not enough to precisely identify the sending subspace, so *Eve* cannot decode the message correctly. However, he can guess the k dimensional sending subspace with the knowledge of l intercepted vectors. The method of guess is also used in [4]. The probability of a successful guess measures the security of subspace code. With the method of combinatorics, we make detailed analyses to the probability in the following.

3.2. Guess Probability

Before analyses, we introduce a counting result of a constant dimensional subspace code. The number of k dimensional subspaces of F_q^n is denoted by $\begin{pmatrix} n \\ k \end{pmatrix}_q$, which is called Gaussian coefficient in combinatorics [19]. It is equal to

$$\begin{pmatrix} n \\ k \end{pmatrix}_q = \frac{\left(q^n-1\right)\left(q^{n-1}-1\right)\cdots\left(q^{n-k+1}-1\right)}{\left(q^k-1\right)\left(q^{k-1}-1\right)\cdots\left(q-1\right)} \tag{3}$$

WLOG, denote the l wiretapped vectors by $\mathbf{V}_1,\cdots,\mathbf{V}_l$, $(l \le k-1)$. Then, we have

Theorem 1: Within the vector space F_q^n, the number of distinct k dimensional subspaces containing $\mathbf{V}_1,\cdots,\mathbf{V}_l$ equals

$$M = \frac{\left(q^{n-l}-1\right)\left(q^{n-l-1}-1\right)\cdots\left(q^{n-k+1}-1\right)}{\left(q^{k-l}-1\right)\left(q^{k-l-1}-1\right)\cdots\left(q-1\right)} \tag{4}$$

Proof: Assume the basis vectors of the k dimensional subspace are $\mathbf{V}_1,\cdots,\mathbf{V}_l$, $\mathbf{V}_{l+1},\cdots,\mathbf{V}_k$. Because $\mathbf{V}_{l+1}$ must take a value other than any linear combination of $\mathbf{V}_1,\cdots,\mathbf{V}_l$, the number of possible choices of $\mathbf{V}_{l+1}$ should be $q^n - q^l$. Similarly, we get the number of possible choices for $\mathbf{V}_i$ $(l+1 \le i \le k)$ and denote it by $N(.)$.

It is listed below.

$$N(\mathbf{V}_{l+1}) = q^n - q^l, N(\mathbf{V}_{l+2}) = q^n - q^{l+1}, \cdots, N(\mathbf{V}_k) = q^n - q^{k-1} \tag{5}$$

Thus, the number of possible k dimensional bases containing $\mathbf{V}_1, \cdots, \mathbf{V}_l$ should be

$$\left(q^n - q^l\right)\left(q^n - q^{l+1}\right)\cdots\left(q^n - q^{k-1}\right) \tag{6}$$

Next, consider a specific k dimensional subspace S_i containing $\mathbf{V}_1, \cdots, \mathbf{V}_l$. If we still denote the basis of S_i as $\mathbf{V}_1, \cdots, \mathbf{V}_l, \mathbf{V}_{l+1}, \cdots, \mathbf{V}_k$, then the number of possible choices of $\mathbf{V}_i$ ($l+1 \le i \le k$), denoted by $N'(.)$, should be

$$N'(\mathbf{V}_{l+1}) = q^k - q^l, N'(\mathbf{V}_{l+2}) = q^k - q^{l+1}, \cdots, N'(\mathbf{V}_k) = q^k - q^{k-1} \tag{7}$$

That is to say for the specific k dimensional subspace S_i, the number of possible choices of $\mathbf{V}_1, \cdots, \mathbf{V}_l, \mathbf{V}_{l+1}, \cdots, \mathbf{V}_k$ is

$$\left(q^k - q^l\right)\left(q^k - q^{l+1}\right)\cdots\left(q^k - q^{k-1}\right) \tag{8}$$

Connecting (6) and (8), the number of distinct k dimensional subspaces containing $\mathbf{V}_1, \cdots, \mathbf{V}_l$ equals

$$M = \frac{\left(q^n - q^l\right)\left(q^n - q^{l+1}\right)\cdots\left(q^n - q^{k-1}\right)}{\left(q^k - q^l\right)\left(q^k - q^{l+1}\right)\cdots\left(q^k - q^{k-1}\right)} = \frac{\left(q^{n-l} - 1\right)\left(q^{n-l-1} - 1\right)\cdots\left(q^{n-k+1} - 1\right)}{\left(q^{k-l} - 1\right)\left(q^{k-l-1} - 1\right)\cdots(q-1)} \tag{9}$$

One may notice that (3) is a special case of (4) with $l = 0$. To calculate the guess probability, we assume the source messages are uniformly distributed, *i.e.*, all k dimensional subspaces are equiprobable. With this assumption, the enemy can successfully guess the sending subspace with the probability of

$$P = \frac{1}{M} = \frac{\left(q^{k-l} - 1\right)\left(q^{k-l-1} - 1\right)\cdots(q-1)}{\left(q^{n-l} - 1\right)\left(q^{n-l-1} - 1\right)\cdots\left(q^{n-k+1} - 1\right)} \tag{10}$$

With the setting of ($n = 8$, $q = 2$, $k = 6$), the probability P is calculated and shown in Figure 4, which shows the probability increases with l. This is an intuitive result, since the more vectors *Eve* intercepts, the easier for him to guess the correct subspace.

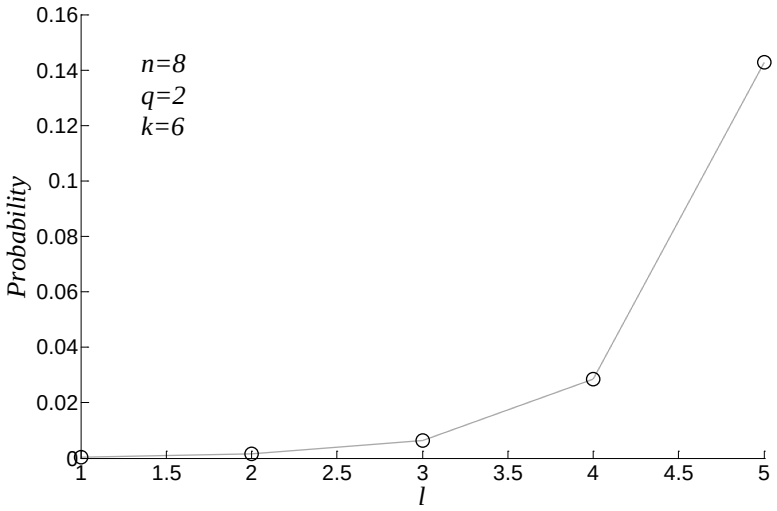

Figure 4. Guess probability P increases with l.

To observe the relation between P and k, set $l = k - 1$. This is corresponding to the case that the number of wiretapped vectors is just one less than the dimension of the subspace code. With this setting, P reduces to

$$P = \frac{(q-1)}{\left(q^{n-k+1}-1\right)} \tag{11}$$

The curve related to (11) is delineated in Figure 5. It shows that P is an increasing function of k. This means the dimension of subspace code should be set as small as possible.

3.3. Information Leakage

Finally, with the notation of information theory, we can calculate the amount of information leakage. Prior to being wiretapped, all k-dimensional subspaces, *i.e.*, all code words, are equiprobable, so the average uncertainty for *Eve* equals the logarithm of the Gauss coefficient. After *Eve* wiretapped $\mathbf{V}_1, \cdots, \mathbf{V}_l$, only M codewords are left with equal probability, which become potential sending codewords. So, the average uncertainty reduces to $\log(M)$. As a result, the information leakage, which is equivalent to the decrease of the average uncertainty, equals

$$\begin{aligned} I(\mathbf{m};\mathbf{y}_A) &= H(\mathbf{m}) - H(\mathbf{m}\,|\,\mathbf{y}_A) = \log\left(\begin{pmatrix} n \\ k \end{pmatrix}_q\right) - \log(M) \\ &= \log\left[\frac{\left(q^n-1\right)\cdots\left(q^{n-l+1}-1\right)}{\left(q^k-1\right)\cdots\left(q^{k-l+1}-1\right)}\right] (\text{bits}/l \text{ vectors}) \end{aligned} \tag{12}$$

4. Comparison and Discussion

Different from perfect security and weak security, the security of subspace code is evaluated by the guess probability. Because there is an amount of information

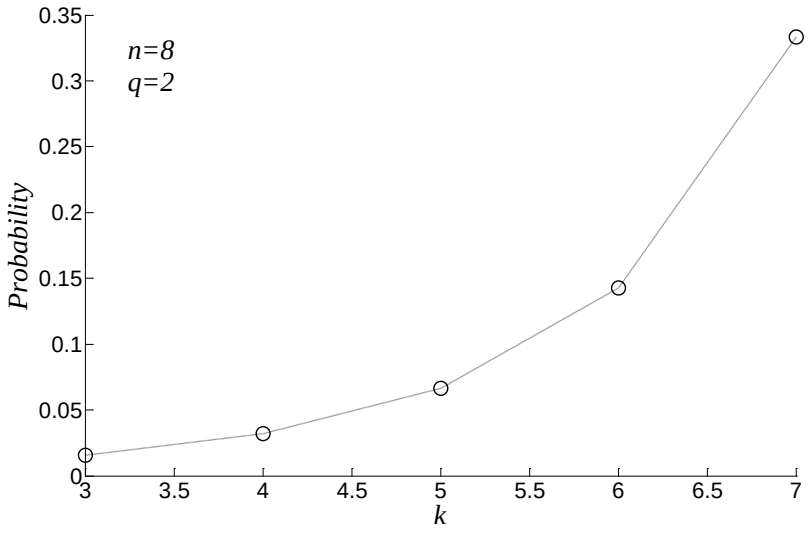

Figure 5. Guess probability P increases with k.

leakage, subspace code is not perfectly secure. Its security performance is not as competent as perfectly secure codes and may be inferior to some weakly secure codes. However, we mention that these schemes achieve security at the cost of extra operations, such as precoding [3] [12], coset code [13], encryption [6] [7] [8] [9], or complicate algorithms [4] [5], etc.

Take [5] as an example. Adeli and Liu designed a LNC protocol to combat to1-WNM, *i.e.*, wiretap on a single edge. Their basic idea is as the following. To prevent any symbol m_i from being exposed on any edge, it is sufficient to force the GCV not to be multiples of a unit vector; Or else, the wiretapped symbol will become a multiple of m_i. To this end, [5] designed a local strategy by assigning LCVs for all intermediate nodes subject to the requirement of no ongoing GCVs being multiples of a unit vector. However, this strategy is very heavy due to a large number of iterations. Still, it is not suitable for mobile networks since the topology has changed before the algorithm converges. More seriously, [5] is only effective to 1-WNM. For an r-WNM, say $r = 2$, [5] is not enough to prevent *Eve* from resolving m_i by wiretapping two symbols from network links.

Compared to [5], subspace code achieves probabilistic security for r-WNM with $r \geq 1$. In **Figure 4**, the point ($l = 1$, $P = 0.0004$) corresponds to 1-WNM. The guess possibility is trivial. Moreover, subspace code is characterized by low complexity. Specifically, the source node just maps a message into a subspace and send the basis vectors of the subspace into the network; An intermediate node implements linear encoding operations just as a general random network coding; The sinks need to calculate the subspace spanned by a number of k received n dimensional independent vectors. It can be done with the method of Gaussian elimination at the complexity of $O(kn)$. The LNC protocol of [5] is compared to subspace code in **Table 1**.

Except for complexity gains, subspace code is more scalable and flexible than many secure coding schemes. For example, most LNC schemes with perfect security or weak security need a private link to share confidential components, such as symmetric key, precoding matrix, hash function or permutation function, etc. This adds extra cost and may not be implementable in some cases. However, there is no need of confidential channels in subspace code. Moreover, many secure coding schemes are only effective to fixed networks. On the contrary, subspace code can work in both fixed and mobile networks, so it is more flexible with the underlying network. The comparison of subspace code with some secure LNC schemes is listed in **Table 2**.

Table 1. Comparison between [5] and subspace code.

Schemes	Performance Metrics		
	Topology	Complexity	Feasibility
[5]	Fixed	High	1-WNM
Subspace Code	Variable	Low	r-WNM

Table 2. Comparison between secure LNC codes.

Schemes	Security	Topology	Method	Private Link
[3] [12] [13] [14]	Perfect	Fixed	Precoding	Need
[6]	Weak	Variable	Encryption	Need
[7]	Weak	Variable	Hash function	Need
[5]	Weak	Fixed	LNC algorithm	No need
[8]	Weak	Variable	Permutation	Need
[9]	Weak	Variable	Permutation	Need
Subspace Code	Basic	Variable	None	No need

5. Conclusion

In this paper, we analyze the security performance of a constant dimensional subspace code against wiretap attacks. The analysis is developed with the method of combinatorics. The attacking capability of the enemy is measured by the number of wiretapped packets and the security is measured by the guess probability. A quantitative solution of the probability is obtained. The result shows that subspace code is not perfectly secure, but it gets probabilistic security with low complexity. Still, subspace code is characterized by high flexibility, no need of private link, and topology independence, etc. In conclusion, subspace network coding is suitable to the security applications with limited computation and moderate security requirement. It has the properties of low complexity, high flexibility and extendibility, as well as little bandwidth consumption, etc. Future work can be done on effectively integrating subspace network coding with existing security techniques, such as encryption, to further strengthen network security.

Acknowledgements

This work is supported in part by NSFC with No. 61471045 and Natural Science Foundation of Liaoning Province with No. 20170540008.

References

[1] Li, S.Y.R., Yeung, R.W. and Cai, N. (2003) Linear Network Coding. *IEEE Transactions on Information Theory*, **49**, 371-381. https://doi.org/10.1109/TIT.2002.807285

[2] Cai, N. and Yeung, R.W. (2002) Secure Network Coding. 2002 *IEEE International Symposium on Information Theory* (*ISIT*'02), Lausanne, 30 June-5 July 2002, 323. https://doi.org/10.1109/ISIT.2002.1023595

[3] Feldman, J., Malkin, T., Stein, C. and Servedio, R.A. (2004) On the Capacity of Secure Network Coding. *Proceeding of the* 42nd *Annual Allerton Conference on Communication, Control, and Computing*, Monticello, VA, 29 Sep-1 Oct 2004, 1-10.

[4] Bhattad, K. and Narayanan, K.R. (2005) Weakly Secure Network Coding. *Proceeding of the First Workshop on Network Coding* (*NetCod*'05), Riva del Garda, April 2005, 281-285.

[5] Adeli, M. and Liu, H. (2013) On the Inherent Security of Linear Network Coding. *IEEE Communications Letters*, **17**, 1668-1671. https://doi.org/10.1109/LCOMM.2013.062113.130478

[6] Vilela, J.P., Lima, L. and Barros, J. (2008) Lightweight Security for Network Coding. 2008 *IEEE International Conference on Communications*, Beijing, 19-23 May 2008, 1750-1754. https://doi.org/10.1109/ICC.2008.336

[7] Adeli, M. and Liu, H. (2009) Secure Network Coding with Minimum Overhead Based on Hash Functions. *IEEE Communications Letters*, **13**, 956-958. https://doi.org/10.1109/LCOMM.2009.12.091648

[8] Zhang, P., Jiang, Y.X., Lin, C., Fan, Y.F. and Shen, X.M. (2010) P-Coding: Secure Network Coding against Eavesdropping Attacks. *Proceeding of* 2010 *IEEE INFOCOM*, San Diego, 14-19 March 2010, 1-9. https://doi.org/10.1109/INFCOM.2010.5462050

[9] Yawen, W., Zhen, Y. and Guan, Y. (2010) Efficient Weakly-Secure Network Coding Schemes against Wiretapping Attacks. 2010 *IEEE International Symposium on Network Coding* (*NetCod*), Toronto, 9-11 June 2010, 1-6. https://doi.org/10.1109/NETCOD.2010.5487671

[10] Cao, Z., Zhang, S., Ji, X. and Zhang, L. (2015) Secure Random Linear Network Coding on a Wiretap Network. *International Journal of Electronics and Communications*, **69**, 467-472. https://doi.org/10.1016/j.aeue.2014.10.018

[11] Liu, G., Liu, B., Liu, X., Li. F. and Guo, W. (2016) Low-Complexity Secure Network Coding against Wiretapping Using Intra Inter-Generation Coding. *China Communications*, **12**, 116-125. https://doi.org/10.1109/CC.2015.7122470

[12] Cai, N. and Yeung, R.W. (2011) Secure Network Coding on a Wiretap Network. *IEEE Transactions on Information Theory*, **57**, 424-435. https://doi.org/10.1109/TIT.2010.2090197

[13] Rouayheb, S.Y.E. and Soljanin, E. (2007) On Wiretap Networks II. 2007 *IEEE International Symposium on Information Theory*, Nice, 24-29 June 2007, 551-555. https://doi.org/10.1109/ISIT.2007.4557098

[14] Silva, D. and Kschsiischang, F.R. (2008) Security for Wiretap Networks via Rank-Metric Codes. 2008 *IEEE International Symposium on Information Theory*, Toronto, 6-11 July 2008, 176-180. https://doi.org/10.1109/ISIT.2008.4594971

[15] Harada, K. and Yamamoto, H. (2008) Strongly Secure Linear Network Coding. *IEICE Transactions Fundamental*, **E91**-**A**, 2720-2728.

[16] Köetter, R. and Kschsiischang, F.R. (2008) Coding for Errors and Erasures in Random Network Coding. *IEEE Transactions on Information Theory*, **54**, 3579-3591. https://doi.org/10.1109/TIT.2008.926449

[17] Roth, R.M. (1991) Maximum-Rank Array Codes and Their Application to Crisscross Error Correction. *IEEE Transactions on Information Theory*, **37**, 328-336. https://doi.org/10.1109/18.75248

[18] Chou, P.A., Wu, Y. and Jain, K. (2003) Practical Network Coding. *Proceeding of the* 41*th Annual Allerton Conference on Communications*, *Controls and Computations*, Monticello, 2-4 October 2003, 1-10.

[19] Van, L.J.H. and Wilson, R.M. (2001) A Course in Combinatorics. 2nd Edition, Cambridge University Press, Cambridge.